REMARKS

Claims 22-29 are in the case and presented for consideration.

Claims 1, 9, 11, 13, 16 and 17 are canceled without prejudice to Applicants' right to pursue the canceled subject matter in a continuing application. Accordingly, rejections with respect to claims 1, 9, 11, 13, 16 and 17 are believed to be moot.

Claim 22 has been amended to better define the claimed invention. Support for the feature "an access privilege proving data storage unit that stores access privilege proving data, the access privilege proving data being created from a private key corresponding to a public key assigned to the requested service and result of a second unique operation" can be found for example on page 4, line 31, to page 5, line 5, page 10, line 31, to page 11, line 7, and page 13, lines 1-5, of the specification.

Newly added claims 27-29 correspond to canceled claims 9, 11 and 13. Accordingly, no new matter has been added

Claims 1, 13, 16, 17, 22-26 are rejected under 35 U.S.C. § 102(e) as being unpatentable over U.S. Patent 6,721,886 to Uskela.

Applicants' claim 22 has been amended to recite as follows:

> A system comprising:
> a server that provides service to a client;
> the server further comprising:
> a public-key storage unit that stores a public key assigned to the service;
> a challenge generator that generates a challenge to be sent from the server to the client after the server receives a request for the service from the client;
> an access privilege verifier that verifies whether a prescribed relationship exists between the challenge and a response, the response being corresponding the challenge and received from the client; and
> the client that requests the service from the server, the client comprises:
> an unique operation executer that executes a first unique operation assigned to the client;

> an access privilege proving data storage unit that stores access privilege proving data, the access privilege proving data being created from a private key corresponding to a public key assigned to the requested service and result of a second unique operation;
>
> a response generator that generates the response to the challenge, the challenge being received from the server;
>
> wherein the response is calculated based on the first unique operation and the access privilege proving data, and
>
> wherein a valid response is not calculated unless the first unique operation coincides with the second unique operation.

The system as claimed in claim 22 is patentably distinguished from Uskela for the reasons which are discussed below. Uskela describes an authentication scheme whereby the service provider sends a random number encrypted with the subscriber's public key as a challenge. See Uskela, col. 5, lines 23-27. The encrypted challenge is deciphered using the subscriber's private key to produce a response. See Uskela, col. 5, lines 27-31. The response is then sent back to the service provider which compares the original random number with the response to determine whether there is a match. See Uskela, col. 5, lines 32-35. In situations where a subscriber requires access to different services, the authentication scheme according to Uskela would require the subscriber to maintain a separate private key that corresponds to each of the different services available to the subscriber. To maintain the integrity and security of the system, the subscriber must keep all the private keys secret. This illustrates a major drawback of the authentication technique as described by Uskela because once the subscriber's private key is compromised or revealed, it would be difficult or perhaps impossible to prevent the unauthorized use of the subscriber's secret key to decrypt the authentication challenges issued by the service provider.

Uskela also fails to disclose or suggest a system whereby the response to a challenge is generated using an access privilege proving data and the first unique operation performed by the client, and whereby the access privilege proving data is created from the private key corresponding to the public key assigned to a particular service of the server being requested by the client using a second unique operation. Therefore, even if the access privilege proving data, which is obtained from the client's private key, is copied by a third party illegally or without approval, the third party will not be able to output the correct response to the server. For instance, the system as claimed in claim 22 only requires one unique operation to be securely stored. To generate the correct response needed by the server to grant access a service requested by the client, the client only need the access privilege proving data units corresponding to each service available to the client, which need not be stored securely.

Based on the foregoing, Applicant maintains that claim 22 recites patentable subject matter, and therefore, withdrawal of the rejection with respect to claim 22 is respectfully requested.

Claims 23-29 depend from claim 22, and therefore include the features of claim 22. Accordingly, for the same reasons given above for claim 22, claims 23-29 also contain patentable subject matter, and therefore, withdrawal of the rejection with respect to claims 23-29 is respectfully requested.

If any issues remain, the Examiner is respectfully invited to contact the undersigned to advance the application to allowance.

Respectfully submitted,

/Chih-Sheng Lin/
Reg. No. 56,402
Attorney for Applicants
ph. (845) 359-7700

Dated: June 21, 2006

NOTARO & MICHALOS P.C.
100 Dutch Hill Road, Suite 110
Orangeburg, New York 10962-2100

Customer No. 21706

F:\TEXT\PATAMD\J355-037US-AMD-DRAFT.wpd